Discussion – Network Visualisation

Filtering at the human level seems to be important

Data mining, algorithmic approaches.
Sensors don't have a broad enough view of what's going on
Attacks don't just happen, sensors don't have perception in order to filter important information

Instead of looking at anomalies, looking at what characterizes the normal working situation.

Only a few ways to become a root user on a UNIX system. Instead of tracking all uses, if you look at tracking only when a user becomes a root user through means other than the prescribed, it can automatically be seen as suspect.

Hard to profile users. It's hard to say what's normal behavior and what's not. Could result in many false positives.

Slow and wide attacks. How are nations sharing information for visualisation. Can't share low level data, too much, what abstraction are they using, passing ontologies as well?
Currently there isn't that much interoperability. Very difficult to share. Distributed visualisation dependent on classification of information. Classic problem with coalition operations, you may have a very good picture but note everyone may be able to see what you're seeing and then miss the details that are important. Political decision – what to make available. Technical – language, common tools and fundamental structures. How do we translate our survival skills developed in this world into the new automated space.

Humans have limited attention. Issue of false alarms – number may not be as important as how difficult they are to deal with. If you are not used to the environment, you may not notice abnormal events.

If you have a tool to identify normal and abnormal events you can apply them to each other.

Auto correlation to highlight significant events

Consistent visual environment – if they know your algorithm, or display, it can make it easier to hack, and may limit your visualisation

If you had all the data it would avoid the possibility of missing something from not having everything available, but would be a flood of data.

Consistency, coherence, and coverage

Visual environment needs to be molded to the tasks that the user has to perform.

Expert systems – cost and performance important

Could it all be one huge neural net?

Taxonomies, how do you address it, and how do you approach it in terms of search engine capabilities in order to retrieve it?

Can a taxonomy be defined when you don't know enough about the domain. Perhaps ontologies are better, as they are meant to evolve. No ontological model will ever be complete. Ensure that the ontology is not written in stone and can be flexible. A problem on this scale may not be able to be taken on at once.

But a framework model is important. Information and knowledge capture is imperative. Scalability is a consideration. Archiving and searching.

If we know how to find fingerprints we won't try to track every single event

Looking at relationships to manage data.

Portals – makes it easier to segment the information. Creates hierarchical views. Allows user to customize their presentation needs.

Portal – allows you to see any information you want through a single window, in the way you want to see it.